

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

OATHER MCCLUNG, et al.,

Plaintiffs,

v.

ADDSHOPPER, INC., et al.,

Defendants.

Case No. 23-cv-01996-VC

**ORDER GRANTING IN PART AND  
DENYING IN PART THE MOTIONS  
TO DISMISS**

Re: Dkt. Nos. 50, 51

The motions to dismiss are granted in part and denied in part. The UCL and CDAFA claims may proceed. The statutory larceny, unjust enrichment, and invasion of privacy claims are dismissed. The CIPA claim asserted by plaintiff Dessart against Every Man Jack is dismissed, but the rest of the CIPA claims may proceed. This ruling assumes the reader is familiar with the facts, the applicable legal standards, and the arguments made by the parties.

1. *Personal jurisdiction.* The complaint adequately alleges specific personal jurisdiction over AddShoppers in California. According to the complaint, the company orchestrates a scheme with thousands of retailers to (1) intercept and collect information that consumers share with those retailers; and (2) use that collection of information to send unwanted emails to the devices of those consumers. Many of the retailers are alleged to be California companies (including the two retailers named as defendants). This case is distinguishable from the recently issued *Briskin v. Shopify, Inc.*, 87 F.4th 404 (9th Cir. 2023). There, Shopify's contractual arrangements with California retailers were for the processing of consumer payments—they were distinct from (and therefore unrelated to, for purposes of specific jurisdiction) the scheme that Shopify allegedly implemented to passively collect information from consumers in California and nationwide. *Id.*

at 413–15. In this case, the alleged contracts between AddShoppers and California retailers are for the express purpose of enabling AddShoppers to collect customer data and conduct unsolicited customer outreach. In other words, the alleged agreements with California companies directly caused the harm. *Contrast id.* at 414 (“There is no such causal relationship between Shopify’s broader California business contacts and Briskin’s claims because these contacts did not cause Briskin’s harm.”).

2. *Article III standing.* The complaint adequately alleges Article III standing against AddShoppers and the two retailer defendants. Misappropriating a person’s browsing activity across a network of thousands of online retailers and using it to barrage that person’s devices with unwanted email communications (particularly without giving the person a way to put a stop to the communications) is the type of intrusion on privacy and seclusion that can be vindicated in the federal courts. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 424–25 (2021); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 598 (9th Cir. 2020); *In re Facebook, Inc., Consumer Privacy Litigation*, 402 F. Supp. 3d 767, 784–87 (N.D. Cal. Sept. 2019). As discussed below, the defendants may ultimately be right that the intrusion here does not confer liability. But for purposes of assessing whether a plaintiff has adequately alleged standing, courts consider the nature and existence of the injury, not the likelihood of success on the merits. The question whether an invasion of privacy is severe enough to confer liability is distinct from whether the injury is concrete and particularized enough to confer standing in federal court.

Given that, the plaintiffs clearly have alleged standing to sue AddShoppers: it orchestrated the scheme and then directly took the injury-causing actions. As for the retailer defendants, standing is a close question. According to the complaint, these retailers played a comparatively small role in the overall scheme. Specifically, the retailers joined the network created by AddShoppers, which caused the plaintiffs to receive unwanted email communications from AddShoppers when they visited the retailers’ websites. But, as described in the complaint, the scheme cannot exist without the participation of the retailers, and the retailers were aware that their participation would cause these intrusions. The ultimate injury is not merely the

dissemination of one unwanted email from one website; it is the aggregation of information about a consumer's browsing history across thousands of retail sites and the systematic dissemination of emails from the AddShoppers' network based upon that information. The knowing participation in this scheme by a retailer is enough to confer standing for a victim of the scheme to sue that retailer in federal court.<sup>1</sup>

3. *Statutory standing.* The complaint adequately alleges statutory standing for the claims against AddShoppers—UCL, CDAFA, statutory larceny—that require an allegation of monetary loss. The Court continues to be skeptical of the plaintiffs' theory that California's statutory standing requirement for these claims can be satisfied simply by alleging that the defendant was unjustly enriched by the misappropriation of personal information. *See Hazel v. Prudential Financial, Inc.*, No. 22-cv-07465-CRB, 2023 WL 3933073, at \*6 (N.D. Cal. June 9, 2023) ("Just because Plaintiffs' data is valuable in the abstract, and because [a company] might have made money from it, does not mean that Plaintiffs have 'lost money or property' as a result."); *see also Facebook Consumer Privacy*, 402 F. Supp. 3d at 784 (holding in the context of Article III standing that, "[a]lthough it's true that each user's information is worth a certain amount of money to Facebook and the companies Facebook gave it to, it does not follow that the same information, when not disclosed, has economic value to an individual user. . . . The plaintiff's economic-loss theory is therefore purely hypothetical").<sup>2</sup> But the complaint also alleges

---

<sup>1</sup> The retailer defendants rely on two cases in which courts found that the plaintiffs did not have standing to sue websites in situations where the plaintiffs' browsing activity was tracked but never tied to their personal information. *Byars v. Sterling Jewelers, Inc.*, No. 22-cv-1456-SB-SP, 2023 WL 2996686, at \*2 (N.D. Cal. April 5, 2023); *Lightoller v. Jetblue Airways Corporation*, No. 23-cv-00361-H-KSC, 2023 WL 3963823, at \*1, \*4–5 (S.D. Cal. June 12, 2023). These cases do not stand for the proposition that a website only causes a privacy injury where it collects the personal information *itself*. The whole idea of AddShoppers' scheme is to tie browsing activity on one site with personal information disclosed on another site, obviating the need for the retailers to do it themselves.

<sup>2</sup> The Ninth Circuit's opinion in *Facebook Internet Tracking* contains a section noting that the "unjust enrichment" theory asserted by the plaintiffs here is sufficient to confer Article III standing. Although it's difficult to tell, this section may also have been intended to convey that the unjust enrichment theory is sufficient to confer statutory standing for claims based on California provisions such as the UCL. However, the Article III analysis in that section of *Facebook Internet Tracking* has been superseded by *TransUnion*, making it even more of a

monetary loss in a more conventional way. Although the allegations could have been set forth more clearly, the complaint creates a reasonable inference that the plaintiffs purchased products from retailers in the network created by AddShoppers, and that they entered AddShoppers's network and received unwanted email communications as a result of those purchases. And the complaint does allege clearly that the plaintiffs would not have purchased products from these retailers had they known that it would subject them to the alleged scheme. Thus, the plaintiffs were denied the benefit of their bargain with these retailers because of AddShoppers's actions. This type of monetary loss is sufficient to confer statutory standing. *See In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation*, 613 F. Supp. 3d 1284, 1301 (S.D. Cal. May 2020) ("Courts in California have consistently held that benefit of the bargain damages represents economic injury for purposes of the UCL."). AddShoppers argues that this theory is inapplicable when the plaintiffs have not transacted directly with the defendant. But there is no basis for that distinction. AddShoppers's alleged scheme is what denied the plaintiffs the benefit of the bargains with the retailers that the plaintiffs did transact with.<sup>3</sup>

Again, whether this alleged injury creates standing to sue the retailer defendants (in addition to AddShoppers) is a closer question. But, as discussed above, although the causal connection between the injury and the retailer defendants' conduct is more attenuated, the retailer defendants' participation in the overall scheme that caused the injury is still sufficient to provide the plaintiffs with standing.

4. *Consent*. The complaint and the materials properly considered at the motion-to-dismiss stage do not establish that the plaintiffs consented to the alleged misappropriation of their data or the subsequent emails. First, the complaint alleges that the cookies that AddShoppers installs

---

stretch to rely on that section as an implicit statement about statutory standing under California law. *See TransUnion*, 594 U.S. at 426–30.

<sup>3</sup> Since the list of retailers that participate in AddShoppers's scheme is not public information, the plaintiffs could not have specifically identified which online purchases provided AddShoppers with their personal information. Nonetheless, the best inference from the complaint is that the plaintiffs bought products from at least one of the retailers on the list.

sync with the user’s device the moment that they access the website—thus, by the time the user even sees the cookie banner, the initial visit has already been tracked and linked to AddShoppers’s dossier of browsing activity and personal information. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at \*2 (9th Cir. May 31, 2022) (unpublished) (concluding that CIPA and state common law claims were not invalid based on retroactive consent as opposed to express prior consent). Second, the plaintiffs allege they never clicked the “Accept” button on the cookie banner. Thus, it cannot be said that the plaintiffs “took an action that unambiguously manifested their assent to be bound by the terms and conditions” of the privacy policies. *Berman v. Freedom Financial Network, LLC*, 30 F.4th 849, 858–59 (9th Cir. 2022).<sup>4</sup>

5. CIPA. The plaintiffs sufficiently allege that the communications were intercepted “in transit” within the meaning of § 631(a). The complaint does more than merely recite the statutory element: it makes specific factual allegations describing how AddShoppers’s cookies intercept the information in real time, and it points to statements allegedly made by AddShoppers about real time transmission. Dkt. No. 60 at 31–32. *Compare Valenzuela v. Keurig Green Mountain, Inc.*, No. 22-cv-09042-JSC, 2023 WL 3707181, at \*5 (N.D. Cal. May 24, 2023) (dismissing CIPA claims where the complaint “does little more than restate the pleading requirement of real time interception”) with *Valenzuela v. Nationwide Mutual Insurance Co.*, No. 2:22-cv-06177-MEMF-SK, 2023 WL 5266033, at \*5 (C.D. Cal. Aug. 14, 2023) (allowing CIPA claims to proceed where the complaint “added detail on how [real time interception] occurs through the code” and “pointed to statements” by the intercepting party). With one exception discussed in the next paragraph, the defendants’ other arguments against the CIPA claims are also unsuccessful, and too weak or undeveloped to merit a response.

One particular CIPA claim must be dismissed: plaintiff Dessart’s claim against Every

---

<sup>4</sup> AddShoppers’s version of the consent argument is even weaker: the fact that AddShoppers has terms of service requiring retailers to have privacy policies that cover AddShoppers’s conduct does not compel the conclusion that AddShoppers enforces those terms, or that its retail clients follow them.

Man Jack. According to the complaint, Dessart’s wife was the one to interact with Every Man Jack’s website, and it was his wife’s communications that were intercepted by AddShoppers on Every Man Jack’s website. Therefore, Every Man Jack did not aid AddShoppers in eavesdropping on Dessart. But this wrinkle does not affect Dessart’s CIPA claim against AddShoppers. The email to Dessart demonstrates that AddShoppers has his personal and contact information, which creates a reasonable inference that—on some other retail website—AddShoppers intercepted Dessart’s communications. Thus, Dessart’s CIPA claim against AddShoppers may proceed.

6. *CDAFA*. The only argument made against the plaintiffs’ CDAFA claims has already been rejected by the Ninth Circuit. In *United States v. Christensen*, the court clarified that CDAFA does not require unauthorized access to information, but rather the unauthorized taking and using of such information. 828 F.3d 763, 789 (9th Cir. 2015). In doing so, the court “rejected the idea that, under CDAFA, technical circumvention [is] necessary.” *Brown v. Google LLC*, 20-cv-3664-YGR, 2023 WL 5029899, at \*19 n.6 (N.D. Cal. Aug. 7, 2023).

7. *Statutory larceny*. The plaintiffs bring a claim under California Penal Code Sections 484 and 496 for statutory larceny. But the allegations in the complaint, and the arguments in the brief, are too sparse. The “personal property” that the plaintiffs assert has been stolen is their personal information. In support of that assertion, the plaintiffs only cite *Calhoun v. Google LLC*, 526 F.Supp.3d 605 (N.D. Cal. March 17, 2021), which allowed a larceny claim to go forward based on the idea that the theft of personal information makes it less valuable to the person it was stolen from. *Id.* at 635. As noted in Section 3, the Court is skeptical of this idea, and it certainly isn’t adequately explained in the complaint, let alone applied to the particular personal information allegedly stolen in this case. On the flip side, even if a complaint fails to explain how personal information has monetary value for the person it’s stolen from, it’s not obvious that this should automatically doom a larceny claim. For example, what if an item of personal property has no market value but tremendous sentimental value—does that really fall outside the coverage of these penal code provisions? But the complaint and the briefs do not touch on any of

this. Moreover, the only provision of the larceny statute that the plaintiffs invoke that has a civil cause of action is § 496(c); that provision provides for “actual damages” as a remedy, but the plaintiffs have not sufficiently alleged that they would be entitled to any recovery. Ultimately, because the plaintiffs have not shown that they could recover under the larceny statute for the theft of their personal information, this claim cannot go forward as pled.

8. *Trespass to chattels*. The plaintiffs agreed to voluntarily dismiss this claim pending further discovery. Dkt. No. 60 at 38 n.16.

9. *Unjust enrichment*. The plaintiffs also assert a standalone claim for unjust enrichment against AddShoppers, which is best construed as a quasi-contract cause of action. *See Katz-Lacabe v. Oracle America, Inc.*, 2023 WL 2838118, at \*10 (N.D. Cal. Apr. 6, 2023). But the plaintiffs have not adequately explained how a quasi-contract can be found between them and AddShoppers on the basis of their purchases from the in-network online retailers (or on the basis of AddShoppers’ acquisition and use of their personal information).

10. *Invasion of privacy*. The claims for invasion of privacy are dismissed because the alleged intrusions are not “highly offensive to a reasonable person.” *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. July 2012). Highly offensive conduct is that which amounts to “an exceptional kind of prying into another’s private affairs.” *Medical Laboratory Management Consultants v. American Broadcast Company*, 306 F.3d 806, 819 (9th Cir. 2002). Even if the allegations in the complaint are true, and even acknowledging that the plaintiffs themselves had strong feelings about the intrusions, they were not so serious as to constitute a violation of the California Constitution or tort law relating to privacy.


11. *Doe defendants*. The two causes of action against John Doe Company defendants are dismissed. It is not sufficiently clear which specific but unnamed retail companies the plaintiffs are suing: All retailers that partner with AddShoppers? All retailers that tracked plaintiffs McClung and Lineberry? The retailers from which McClung and Lineberry made purchases that opted them into AddShoppers’s network? Given this uncertainty, the claims against the Doe defendants do not allege sufficient facts to state a claim.

\*\*\*

Discovery may move forward immediately on the surviving claims. All dismissals are with leave to amend. If the plaintiffs wish to file an amended complaint to attempt to cure the defects in the claims that have been dismissed, they must do so within 14 days. However, as mentioned at the hearing, if the plaintiffs wish simply to proceed on the surviving claims, and if discovery on the surviving claim gives them a good-faith basis to reassert the dismissed claims, they are free to seek leave to amend the complaint at that time.

**IT IS SO ORDERED.**

Dated: January 17, 2024

---

VINCE CHHABRIA  
United States District Judge